REMARKS

Applicant appreciates the Examiner's attention to this application.

This response amends claims 1, 13, 25, and 37. Claims 1, 13, 25, and 37 are the pending independent claims. Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested.

ARGUMENT

The Office Action includes claim rejections based on 35 U.S.C. §§ 102(e) and 103(a). Applicant respectfully traverses those rejections. However, in order to avoid the additional delays and expenses frequently associated with the appeal process, this response amends the independent claims to clarify what is meant by the term "isolated execution mode." To the extent that the rejections might be applied to the claims, as amended by this response, Applicant respectfully traverses.

35 U.S.C. § 102(e)

The Office Action rejects claims 1-6, 10-18, 22-30, 34-42, and 46-48 as being anticipated by U.S. patent no 6,327,652 to Paul England et al. (Hereinafter "England").

For a valid rejection under 35 U.S.C. § 102, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." (MPEP § 2131.01, quoting from Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)).

As explained in Applicant's previous response, England pertains to a method for identifying the operating system running on a computer, based on "an identity associated with an initial component for the operating system, combined with identities of additional components that are loaded afterwards." In particular, after digital signatures for each component are validated, the operating system (referred to as a "digital rights management operating system" or "DRMOS") may assume a "trusted identity." (Abstract.) As far as it goes, England appears to describe reasonable facets of a possible approach to supporting digital rights management.

The present application involves technology with embodiments that could also be applied in the arena of digital rights management. However, the present application, and in particular the pending claims, involve many details that England does not disclose. For instance, claim 37 pertains to a system that uses an operating system nub key (OSNK) to protect usage of a subset of a software environment, and claim 37 recites that the operation of "protecting usage" involves "encrypting a value while operating in isolated execution mode" and/or "decrypting an encrypted value while operating in isolated execution mode." Thus, claim 37 recites a system in which "isolated execution mode" is used to protect usage of a subset of a software environment.

Applicant's previous response pointed out that the Detailed Description of the present application describes "isolated execution mode" as a mode of operation in which the platform allows access to a region of system memory that is protected by the platform hardware. Such regions of memory may be referred to as "isolated memory areas" or simply "isolated memory." The platform hardware prevents access to isolated memory when the system is not in isolated execution mode (e.g., when the system is in "normal execution mode"). Furthermore, isolated execution mode is not to be confused with conventional privilege rings. For example, as explained in greater detail in the detailed description, a platform that supports a "normal execution mode" and an "isolated execution mode" may also support privilege rings within the normal execution mode, as well as privilege rings within the isolated execution mode. (FIGs. 1A-1C and page 3, line 8, through page 10, line 27.)

Furthermore, this response amends the independent claims to explicitly describe certain technical features that relate to isolated execution mode. For instance, claim 37 pertains to a system comprising a processor capable of operating in "an isolated execution mode within a ring 0 operating mode," wherein the processor also supports (a) one or more higher ring operating modes, as well as (b) "a non-isolated execution mode within at least the ring 0 operating mode."

England makes no mention of isolated execution mode, let alone "an isolated execution mode" and a "non-isolated execution mode," both of which may operate with a ring 0 operating mode. *A fortiori*, England does not disclose either encrypting a value or decrypting a value "while operating in isolated execution mode." England therefore does not anticipate claim 37. For the same or similar reasons, England also does not anticipate claim 1, 13, and 25, each of which involves operations to be executed with a processor or platform in isolated execution mode. England therefore does not anticipate any of the independent claims. Accordingly, since each dependent claim implicitly includes the features of its parent claim or claims, England does not anticipate any of the pending claims.

35 U.S.C. § 103(a)

The Office Action rejects claims 7-8, 19-20, 31-32, and 43-44 as being unpatentable over England. Each of those claims depends ultimately from an independent claim that involves encryption and/or decryption to be performed "while operating in isolated execution mode." As indicated above, the independent claims also recite various technical features that relate to isolated execution mode. For instance, claim 37 pertains to a system comprising a processor capable of operating in "an isolated execution mode within a ring 0 operating mode," wherein the processor also supports (a) one or more higher ring operating modes, as well as (b) "a non-isolated execution mode within at least the ring 0 operating mode."

England does not disclose or suggest either encrypting a value or decrypting a value while operating in "isolated execution mode," as that term is explained in the independent claims. In fact, England does not disclose or suggest performing any kind of operations in isolated execution mode. England does not mention isolated execution mode at all. Consequently, England does not render any of the pending claims obvious.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims. For these and other reasons, all pending claims are allowable.

INFORMATION DISCLOSURE STATEMENTS

As indicated in the previous response, Applicant has not received confirmation of consideration of the following Information Disclosure Statements (IDSs):

(a) an IDS that was submitted on April 5, 2002, listing 21 references on two pages;

(b) an electronic IDS (eIDS) that was submitted on August 20, 2003; and

(c) an eIDS that was submitted on December 16, 2003.

In addition, Applicant has not received confirmation of consideration of the following IDS:

(d) an IDS that was submitted on January 12, 2005.

Applicant respectfully requests confirmation that all references listed in those IDSs have been considered.

CONCLUSION

In view of the foregoing, claims 1-8, 10-20, 22-32, 34-44, and 46-48 are all in condition for allowance.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: February 16, 2005

/ Michael Barre /
Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 732-3927

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026